

Sub  
a1

652220-1624260

CLAIMS

1. A method for inspecting an encrypted data stream being transferred over a network between two endpoints, the data stream being encrypted using a session key known to both endpoints, the method comprising:

securely transferring the session key from one of the endpoints to an intermediary having access to the encrypted data stream;

decrypting the encrypted data stream at the intermediary using the session key; and

inspecting the data stream following decryption.

2. A method as recited in claim 1, wherein securely transferring comprises:

encrypting the session key using a public key associated with the intermediary; and

sending the encrypted session key to the intermediary.

3. A method as recited in claim 1, wherein securely transferring comprises:

encrypting the session key using a public key associated with the intermediary;

signing the encrypted session key using a private key associated with the intermediary; and

sending the signed and encrypted session key to the intermediary.

1           4.    A method as recited in claim 1, further comprising storing the data  
2 stream at the intermediary.

3  
4           5.    A method for inspecting an encrypted data stream being transferred  
5 over a network between two endpoints and via an intermediary, the data stream  
6 being encrypted using a session key known to both endpoints, the method  
7 comprising:

8               storing a public key from a public/private key pair associated with one of  
9 the endpoints at a key storage;

10              storing a public key from a public/private key pair associated with the  
11 intermediary at the key storage;

12              obtaining, at said one endpoint, the intermediary's public key from the key  
13 storage;

14              encrypting, at said one endpoint, the session key using the intermediary's  
15 public key to produce an encrypted session key;

16              encrypting, at said one endpoint, the encrypted session key using a private  
17 key from the public private key pair associated with said one endpoint to produce  
18 a signed encrypted session key;

19              passing the signed encrypted session key to the intermediary;

20              obtaining, at the intermediary, the one endpoint's public key from the key  
21 storage;

22              decrypting, at the intermediary, the signed encrypted session key using the  
23 one endpoint's public key to return the encrypted session key;

24              decrypting, at the intermediary, the encrypted session key using the  
25 intermediary's private key to return the session key; and

1 using the session key at the intermediary to decrypt the encrypted data  
2 stream.

3  
4 6. In a network system in which an encrypted data stream is transferred  
5 over a network between two endpoints and via an intermediary, the data stream  
6 being encrypted using a session key known to both endpoints, computer-readable  
7 media at one of the endpoints and at the intermediary storing computer-executable  
8 instructions for performing the method as recited in claim 5.

9  
10 7. In a network system having an external client that exchanges  
11 encrypted data with an external client over a network and through a firewall  
12 intermediate of the internal and external clients, the encrypted data being  
13 encrypted using a session key known to the internal and external clients, a method  
14 executed at the firewall comprising:

15 receiving an encrypted and signed session key from the internal client, the  
16 encrypted and signed session key bearing a digital signature of the internal client;

17 authenticating the digital signature as belonging to the internal client;

18 decrypting the session key; and

19 decrypting the encrypted data being exchanged between the internal and  
20 external clients using the session key.



the internal client being configured to securely transfer the session key to the intermediary; and

the intermediary being configured to decrypt the data using the session key and to inspect the data.

13. A network system as recited in claim 12, wherein the internal client encrypts the session key prior to sending it to the intermediary.

14. A network system as recited in claim 12, wherein the internal client encrypts and signs the session key prior to sending it to the intermediary.

15. A network system as recited in claim 12, wherein the intermediary stores the data in unencrypted form.

16. A software architecture for a network system having two endpoints that exchange encrypted data over a network and through an intermediary, the encrypted data being encrypted using a session key known to the endpoints, comprising:

endpoint-resident code to encrypt the session key using a public key from a public/private key pair associated with the intermediary and to sign the encrypted session key with a digital signature, the endpoint-resident code being capable of sending the signed and encrypted session key to the intermediary; and

intermediary-resident code to authenticate the digital signature and decrypt the encrypted session key using a private key from the public/private key pair associated with the intermediary, the intermediary-resident code using the session

1 key to decrypt the encrypted data as it is being exchanged between the two  
2 endpoints.

3  
4 17. A software architecture as recited in claim 16, wherein  
5 intermediary-resident code inspects the data in unencrypted form.

6  
7 18. A software architecture as recited in claim 16, wherein  
8 intermediary-resident code stores the data in unencrypted form.

9  
10 19. In a network system having an external client that exchanges  
11 encrypted data with an external client over a network and through a firewall  
12 intermediate of the internal and external clients, the encrypted data being  
13 encrypted using a session key known to the internal and external clients,  
14 computer-readable media distributed at the internal client and the firewall storing  
15 computer-executable instructions for:

16 encrypting the session key at the internal client;  
17 signing the encrypted session key with a digital signature associated with  
18 the internal client;  
19 passing the signed and encrypted session key to the intermediary;  
20 authenticating, at the intermediary, the digital signature of the internal  
21 client;  
22 decrypting the session key at the intermediary;  
23 decrypting, at the intermediary, the encrypted data using the session key;  
24 and  
25 inspecting the data in route between the internal and external clients.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

20. *apparatus*

In a network system in which an encrypted data stream is transferred over a network between two endpoints and via an intermediary, the data stream being encrypted using a session key known to both endpoints, computer-readable media at one of the endpoints and at the intermediary storing computer-executable instructions for:

securely transferring the session key from one of the endpoints to an intermediary having access to the encrypted data stream;

decrypting the encrypted data stream at the intermediary using the session key; and

inspecting the data stream following decryption.